PATENT
Attorney Docket No.: 16869B-105700US
Client Ref. No.: HAL308
(340400457US01)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

NOBUYUKI OSAKI

Application No.: 10/799,086

Filed: March 11, 2004

For: METHOD AND APPARATUS FOR CRYPTOGRAPHIC CONVERSION IN A DATA STORAGE SYSTEM

Customer No.: 20350

Examiner: Unassigned

Technology Center/Art Unit: 2131

Confirmation No.: 8546

PETITION TO MAKE SPECIAL FOR NEW APPLICATION UNDER M.P.E.P. § 708.02, VIII & 37 C.F.R. § 1.102(d)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner is authorized to charge the petition fee of $130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430.

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

05/11/2005 SMINASS1 00000001 201430 10799086

01 FC:1202 150.00 DA
02 FC:1201 200.00 DA

(c) Pre-examination searches were made of U.S. issued patents, including a classification search and a foreign patent database search. The searches were performed on or around March 16, 2005, and were conducted by a professional search firm, Mattingly, Stanger & Malur, P.C. The classification search covered Class 380 (subclasses 36, 37, and 42) and Class 713 (subclasses 160, 162, 165, 189, 193, and 200). Because of the large size of these subclasses, keywords were used to narrow of number of documents returned. The foreign patent database search was conducted using Espacenet database and Japanese patent database. The inventors further provided five references considered most closely related to the subject matter of the present application (see references #10-14 below), which were cited in the Information Disclosure Statement filed with the application on March 11, 2004.

(d) The following references, copies of which are attached herewith, are deemed most closely related to the subject matter encompassed by the claims:

(1) U.S. Patent No. 5,548,648;

(2) U.S. Patent No. 5,742,686;

(3) U.S. Patent No. 5,987,572;

(4) U.S. Patent No. 6,570,989 B1;

(5) U.S. Patent Publication No. 2001/0023484 A1;

(6) U.S. Patent Publication No. 2003/0126451 A1;

(7) U.S. Patent Publication No. 2003/0188178 A1;

(8) U.S. Patent Publication No. 2004/0250097 A1;

(9) U.S. Patent Publication No. 2005/0021986 A1;

(10) U.S. Patent No. 5,940,507;

(11) U.S. Patent No. 5,677,952;

(12) U.S. Patent No. 5,235,641;

(13) U.S. Patent No. 5,208,813; and

(14) International Patent Publication No. WO02/093314 A2.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to storage systems and a cryptographic storage technique to provide secure long term retention of data and, more particularly, to a technique for encrypted data storage in a storage system.

Independent claim 1 recites a method for encrypted data storage in a storage system comprising converting blocks of data to produce corresponding converted blocks of data, wherein a converted block of data is encrypted with cryptographic criteria; receiving a read request during the converting in order to access read data from the storage system and in response thereto accessing the read data from at least one decrypted block of data, wherein if the read data is stored in a converted block of data, then decrypting the read data using the cryptographic criteria to produce the at least one decrypted block of data.

Independent claim 9 recites, in a storage system including a storage device, the storage system being coupled to a host device via a network, a method for storing encrypted data comprising converting first data blocks of the storage system to produce corresponding second data blocks, including encryption with cryptographic criteria to produce the second data blocks and replacing each first data block with a corresponding second data block thereof; and accessing read data from the storage device in response to a read request from the host device, including reading a third data block and decrypting the third data block with the cryptographic criteria if the third data block is one of the second data blocks, to return the decrypted third data block to the host device. The step of accessing read data is performed during the step of converting.

Independent claim 15 recites a storage system comprising a storage component; and a cryptographic component in data communication with the storage component and operable to convert unconverted blocks of data stored thereon to produce corresponding converted blocks of data, each converted block of data replacing a corresponding unconverted block of data thereof on the storage component and in the same location as a corresponding unconverted block thereof. The cryptographic component is further operable to receive read and write requests for data stored on the storage component,

while unconverted blocks of data are converted to converted blocks of data. The cryptographic component is further operable to process a read request by accessing read blocks associated with the read request from the storage component, wherein if a read block is unconverted, then performing a first cryptographic process on the read block to produce an unencrypted read block, wherein if the read block is converted, then performing a second cryptographic process on the read block to produce the unencrypted read block. The cryptographic component is further operable to process a write request by writing one or more write blocks associated with the write request from the storage component, wherein if a write block is to be written to a block location that contains an unconverted block, then performing the first cryptographic process on the write block prior to writing the write block, wherein if a write block is to be written to a block location that contains a converted block, then performing the second cryptographic process on the write block prior to writing the write block.

Independent claim 21 recites a method for storing and accessing data on a storage system, comprising receiving from a host device file-level I/O requests; and converting blocks of data stored in the storage system, including for each block of data: performing a first decryption of the block of data to produce an unencrypted block of data, the block of data being encrypted by a first encryption; performing a second encryption of the unencrypted block of data to produce an encrypted block of data; and overwriting the block of data. The method further comprises, during the converting, receiving and servicing a file-level read request; and during the converting, receiving and servicing a file-level write request. Servicing the file-level read request comprises producing one or more block-level read operations; and decrypting a corresponding block of the block-level read operation with either the first or second decryption depending on how the block was encrypted. Servicing the file-level write request comprises producing one or more block-level write operations; encrypting a corresponding block of data of the block-level write operation with the first encryption, if the block-level write operation is targeted to a block location in the storage system containing data that was encrypted with the first encryption; and encrypting the corresponding block of data of the block-level write operation with the second encryption, if the block-level write operation is targeted to a block location in the storage system containing data that was encrypted with the second encryption.

Independent claim 30 recites, in a storage system including a storage device, the storage system being coupled to a host device via a network, a method for storing encrypted data comprising converting first data blocks of the storage system to produce corresponding second data blocks, including encryption with cryptographic criteria to produce the second data blocks and replacing each first data block with a corresponding second data block thereof; receiving a read request from the host device; and returning third data block to which one of the second data blocks is decrypted with the cryptographic criteria. The receiving a read request and the returning third data block are performed during the converting first data blocks.

One of the benefits that may be derived is an efficient encryption scheme with reduced overhead.

B. Discussion of the References

None of the references disclose encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30. For instance, claim 1 recites converting blocks of data to produce corresponding converted blocks of data; and receiving a read request during the converting in order to access read data from the storage system and in response thereto accessing the read data from at least one decrypted block of data. Claim 9 recites accessing read data from the storage device in response to a read request from the host device during the step of converting first data blocks of the storage system to produce corresponding second data blocks including encryption with cryptographic criteria. Claim 15 recites a cryptographic component that is operable to receive read and write requests for data stored on the storage component, while unconverted blocks of data are converted to converted blocks of data. Claim 21 recites converting blocks of data stored in the storage system including encryption; and during the converting, receiving and servicing a file-level read request and receiving and servicing a file-level write request. Claim 30 recites converting first data blocks of the storage system to produce corresponding second data blocks including encryption; receiving a read request from the host device; and returning third data block to which one of the second data blocks is

decrypted with the cryptographic criteria, wherein receiving a read request and returning third data block are performed during converting first data blocks.

1. U.S. Patent No. 5,548,648

The patent to Yorke-Smith, US 5,548,648, discloses a method and system for encrypting data comprising a plurality of data segments divided into a plurality of encrypted data blocks and associated control blocks. The system selects for each data segment an encryption function and means for encrypting for each data segment the data segment using the selected encryption function to form an encrypted data segment. Each control block includes the information necessary to decrypt the data contained in the encrypted data block.

The reference provides a simple encryption method. It fails to teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

2. U.S. Patent No. 5,742,686

The patent to Finley, US 5,742,686, discloses a method and apparatus for the dynamic encryption of information such as data consisting of a random access memory containing encryption and decryption programs and the information to be encrypted and decrypted. The method and apparatus includes an encryption processor executing the encryption and decryption programs, with the encryption and decryption programs being a code set whose members are distinct encryption/decryption codes executed serially by the encryption processor to encrypt and decrypt the information. See, e.g., Abstract; and column 2, lines 9-61.

The reference is directed to dynamic encryption of data. It does not, however, teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

3. U.S. Patent No. 5,987,572

The patent to Weidner et al., US 5,987,572, discloses a method and apparatus that utilizes a dynamic encryption interface located between a processor and a memory. First, it is determined whether or not a memory access request is being made. If a memory access request is being made, then it is determined whether the address location being accessed is greater than a pointer value. If the address location being accessed is greater than a pointer value, then the data is encrypted or decrypted using a first key. If the address location being accessed is less than a pointer value, then the data is encrypted or decrypted using a second key. Then the processor determines whether or not the memory access the request is still active. If the memory access request is not active, then the data is read out from the memory location identified by the pointer value. The data that is read is decrypted using a first key, and the data is encrypted using a second key. The encrypted data is written back to the memory location address indicated by the pointer value. See, e.g., Abstract; and column 2, lines 16-31; and column 5, lines 60-64.

The reference discloses a dynamic encryption interface disposed between a process or and a memory and configured to dynamically encrypt the contents of the memory. It is not directed to encrypted data storage in a storage system. Nor does it teach receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

4. U.S. Patent No. 6,570,989 B1

The patent to Ohmori et al., US 6,570,989, discloses a cryptographic processing apparatus for encrypting/decrypting data in units of blocks, on a block by block basis, based on a secret key. The invention also includes a cryptographic processing method used in the cryptographic processing apparatus, and a storage medium storing a cryptographic processing program for the cryptographic processing method. See, e.g., Abstract; and column 7, lines 27-35.

The reference is directed to a cryptographic processing apparatus that cryptographically processes input data using a plurality of sets of substitution data to generate output data, to reduce the amount of substitution table data and the frequency of generation of

substitution table data. It does not, however, teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

5. U.S. Patent Publication No. 2001/0023484 A1

The published patent application to Ichimura, US 2001/0023484, discloses a transmission apparatus for encrypting a plurality of data blocks and transmitting the encrypted data blocks. The apparatus includes a data inserting means for inserting additional data into the data blocks that are randomly selected among a sequence of data blocks composing a stream of the main data. An encryption means is also included for encrypting the sequence of data blocks after the processing is carried out by the additional data inserting means to insert the additional data. A transmission means transmits the sequence of data blocks encrypted by the encryption means. See, e.g., Abstract; and paragraphs [0021]-[0031].

The reference is directed to preventing transmitted data from being decrypted with ease. It does not teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

6. U.S. Patent Publication No. 2003/0126451 A1

The published patent application to Gorobets, US 2003/0126451, discloses a method for processing data where the data is encrypted before being written to a non-volatile memory where the data cannot be accessed without decryption in the case of when a direct physical access to the memory is made to the non-volatile memory. See, e.g., Abstract; and paragraphs [0010]-[0012].

The reference fails to teach receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

7. U.S. Patent Publication No. 2003/0188178 A1

The published patent application to Strongin et al., US 2003/0188178, discloses a memory, system, and method for providing security for data stored within a memory and arranged within a plurality of memory regions. The memory includes at least one storage location and an encryption/decryption unit for encrypting and decrypting data. The storage location receives a block of data and a corresponding encryption indicator for the block of data. The block of data corresponds to a selected memory region. The encryption indicator indicates whether the data corresponding to the selected memory region is encrypted. The encryption/decryption unit decrypts the block of data dependent upon the encryption indicator before it is stored in the storage location. See, e.g., Abstract; and paragraphs [0019]-[0021].

The references relates to region-granular, hardware-controlled memory encryption. It does not teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

8. U.S. Patent Publication No. 2004/0250097 A1

The published patent application to Cheung et al., US 2004/0250097 discloses a method and system for the transfer of a block of data from a first memory location to a second memory location. The data may be encrypted or decrypted, or bypassed, depending on the mode of selection. In the encryption mode, the data may be buffered, encrypted, and then stored in the second memory location. In the decryption mode, the transferred data may be buffered, decrypted, and then stored in the second memory location. In the bypass mode, the data may be buffered and then stored in the second memory location. See, e.g., Abstract; and paragraphs [0008] and [0027]-[0030].

The reference fails to teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

9. U.S. Patent Publication No. 2005/0021986 A1

The published patent application to Graunke et al., US 2005/0021986, discloses a method and apparatus for memory encryption with reduced decryption latency. The method includes reading an encrypted data block from memory, and regenerating a keystream used to encrypt the data block according to one or more stored criteria of the encrypted data block. Once the encrypted data block is read, the encrypted data block is decrypted using the regenerated keystream. See, e.g., Abstract; and paragraphs [0001] and [0022].

The reference relates to performing memory encryption without exacerbating memory latency between the processor and memory. It does not, however, teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

10. U.S. Patent No. 5,940,507

This patent discloses an information processing system providing archive/backup support with privacy assurances by encrypting data stored thereby. Data generated on a source system 8 is encrypted, the key used thereby is separately encrypted, and both the encrypted data 20 and encrypted key 24 are transmitted to and maintained by a data repository system 30. The repository system receives only the encrypted data and key, while the source system retains the ability to recover the key and in turn, the data. The source system is therefore assured of privacy and integrity of the archived data by retaining access control yet is relieved of the physical management of the warehousing medium.

The reference relates to encryption key management in an information processing system providing archive/backup support with privacy assurances by encrypting data stored. It does not teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

11. U.S. Patent No. 5,677,952

The patent relates to a method, using a secret key, to protect information in a storage disk of a computer, where the secret key is derived from a password entered into the computer by an authorized user. The method begins by applying a length-increasing pseudorandom function to the secret key and an index to generate a pseudorandom bit string having a length that is a function of the size of a sector of the storage disk. The sector is associated or otherwise identified by the index used by the pseudorandom function to generate the pseudorandom bit string. The pseudorandom bit string is then used to encrypt and decrypt data accesses to and from the sector. See column 4, line 50 to column 5, line 3.

The reference discloses the use of a pseudorandom bit string (keys derived from password entered) to encrypt and decrypt data accesses to and from a sector of the storage disk. It does not, however, teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

12. U.S. Patent No. 5,235,641

This patent relates to an information processing system having an upper rank apparatus 1 and an external storage device 12 which performs transmission and reception of data between the storage device and the upper rank apparatus. At least one of encryption and decryption of the data by use of an algorithm controlled by a desired data key is performed in the external storage device (e.g., cryptographic adapter 5), while generation, encryption and decryption of the data key are performed on the upper rank apparatus side. By this configuration, the burden of the upper rank apparatus is largely reduced and the secrecy of data stored in the external storage device can be surely kept without spoiling the throughput of the whole system.

The reference discloses a file encryption scheme. It does not, however, teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

13. U.S. Patent No. 5,208,813

The patent discloses a method for on-line reconstruction of a failed storage unit in a redundant array system. After providing a replacement storage unit for the failed storage unit, reconstruction begins for each data stripe in the array. General reconstruction consists of applying an error-correction operation (such as an XOR operation on data blocks and a corresponding parity block) to the data blocks from the remaining storage units in the redundancy group, and storing the result in the corresponding block of the replacement storage unit. If a Read operation is requested by the CPU for a data block on the replacement storage unit, then a concurrent Read task is executed which reconstructs the stripe containing the requested data block. If a Read operation is requested by the CPU for a data block not on the replacement storage unit, a concurrent Read task is executed which performs a normal Read. If a Write operation is requested for any data block, then a concurrent Write task is executed which performs a Read-Modify-Write sequence in the general case (the Read operation being performed in accordance with the above rules).

The reference relates to on-line reconstruction of a failed redundant array system. It fails to teach encrypted data storage in a storage system including receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

14. International Patent Publication No. WO02/093314 A2

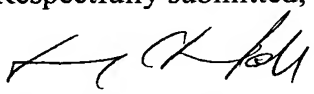
This reference relates to an encryption based security system for network storage that separates the ability to access storage from the ability to access the stored data. This is achieved by keeping all the data encrypted on the storage devices. Logically, the system comprises a device that has two network interfaces: one is a clear text network interface that connects to one or more clients, and the other is a secure network interface that is connected to one or more persistent storage servers. Functionally, each network interface supports multiple network nodes. That is, the clear text network interface supports multiple client machines, an the secure network interface supports one or more storage servers.

The reference provides a network element 20 for encryption/decryption. As such, the reference does not disclose encrypted data storage in a storage system. Nor does it

teach receiving a read request to access read data from the storage system or accessing read data in response to a read request during converting blocks of data to produce corresponding converted blocks of data, as recited in independent claims 1, 9, 15, 21, and 30.

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,



Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
RL:rl
60480968 v1